USAWC STRATEGY RESEARCH PROJECT

SAFEGUARDING MILITARY CRITICAL TECHNOLOGIES

by

Colonel Bryan S. Goda
United States Army

James Downey
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 MAR 2005		-

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Safeguarding Military Critical Technologies	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Bryan Goda	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**36**	

ABSTRACT

AUTHOR: Colonel Bryan S. Goda

TITLE: Safeguarding Military Critical Technologies

FORMAT: Strategy Research Project

DATE: 18 March 2005 PAGES: 36 CLASSIFICATION: Unclassified

One of the basic characteristics of virtually every system in the U.S. military is the utilization of superior technology. Technology allows our systems to see farther, be more accurate, process more information, and shorten the decision making cycle. Technological advantages allow the U.S. military to fight even when outnumbered in any conditions and win.

Unfortunately, our potential adversaries recognize our technological superiority and seek ways to undermine it. This paper examines how military critical technology is created and reviews how poorly we have done protecting our technology in the past. The current system of governmental agencies assigned to protect military critical technologies will be examined and numerous improvements will be discussed.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to acknowledge COL Andre Sayles who helped me get into the Army War College. Without his persistence, this paper would not have been possible. I would also like to acknowledge the invaluable assistance of my advisor, Dr. Jim Downey, for helping me steadily progress in the creation of this Strategic Research Project. Dr. Gabriel Marcella was instrumental in the initial research beginning in course two. I would like to thank my wife Gloria who has been an outstanding Army wife for the past 18 years. Finally I would like to acknowledge the fantastic members of Seminar 4, who helped make my year at the Army War College one of the best in my Army career.

LIST OF ILLUSTRATIONS

LIST OF TABLES

SAFEGUARDING MILITARY CRITICAL TECHNOLOGIES

TECHNOLOGICAL SUPERIORITY

> Our enemy exploited our confidence in our technological superiority by using this arrogance against us with great success. By jamming and reprogramming our Global Positional System (GPS) satellites, our smart munitions and Tomahawk guided missiles missed their targets, often by over 5km. Our communications satellites were also rendered ineffective and many units were out of communication for days at a time. Our laser rangefinders on our M1 tanks were jammed and our main gun rounds were effective only when distances were less than 1000M. This created far greater numbers of U.S. casualties due to the shorter engagement ranges. A computer virus enabled our enemy to shut down our communications network during the opening phases of the war. This virus was embedded by a foreign subcontractor. If only we had paid more attention in protecting our technologies, this war would have been far less costly.
>
> - Hypothetical After Action Report from the Next War

Military Critical Technologies (MCT) is a compendium of goods and technologies that the Department of Defense (DoD) assesses would permit significant advances in the development and production of the military capabilities of our potential adversaries. Our technological superiority supports our national military strategy to field the most potent military force in the world. This superiority allows our military to move, shoot, and communicate with greater speed, accuracy, and distance than any other military force. Potential adversaries are actively pursuing ways to counter this technological superiority which was demonstrated in Operations Enduring Freedom and Iraqi Freedom. This paper will examine how MCT is created, identify the current polices in place to protect MCT, discuss risk assessment, and provide recommendations to improve the safeguarding of MCT. This paper will also highlight the intelligence reform recommendations from the 9-11 Commission as a model for government agency reform that can be applied to MCT protection.

The 19 areas of MCT range from biological systems to information warfare to nuclear systems (Table 1).[1] MCT spans a wide array of capabilities and is often in the forefront of technological discovery. Advances in MCT mainly occur in academia, industry, and research programs. Our academic environment encourages the free exchange of new ideas, which runs contrary to the safeguarding of new technology. U.S. companies that produce MCT are moving towards globalization, which makes it more difficult to safeguard MCT in a foreign environment. Research programs publish their discoveries in open journals to gain notoriety and funding. Often the need for secrecy directly conflicts with the normal MCT research environment.

Military Technology	Overview	Example Capability
Aeronautics Systems	Aircraft, Gas Turbine Engine	Combustion >2800 ^{0} F
Armaments, Energetic Materials	Ammo, Bombs, Mines	Kinetic Penetration >400mm
Chemical and Biological System	Chem Bio Detection, Decon	Protection for 24hrs against all known liquid chemical agents
Directed Energy Systems	High Energy Laser, Particle Beams	>20KW Laser
Electronics	New Generation Microchips	Signal Processor > 1GHz
Ground Systems	Sensors, Advanced Diesel Engines	Power Output >750kW
Guidance, Navigation, and Control	GPS	<1M 3D Accuracy
Information Systems	Data Proc, Info Storage	4 hrs for 72 hr weather forecast
Information Warfare	EW and Hacking	Memory Speed >200MHz
Processing and Manufacturing	Production of equipment	
Materials	Armor, Anti Armor	Body Armor, stop AK47 at 100m
Nuclear Systems	Fission	U235 enrichment to 90%
Sensors and Lasers	Acoustic, Optical Sensor	Locate a direct fire weapon with 10m accuracy out to 500m

TABLE 1. SELECTED EXAMPLES OF MILITARY CRITICAL TECHNOLOGIES

THE DESIRABILITY OF MCT

MCT is a multi-billion dollar industry. Companies involved in supplying MCT often seek an advantage over their competitors in the volatile MCT market (Table 2). Our potential adversaries know our capabilities and seek ways to overcome our technological advantages.

Seeker of MCT	Methods of Attainment	Reasons for Seeking
Rival Companies	Industrial Spying Reverse Engineering	Market Competition Save Research Funds
Foreign Governments	Spies Direct/Indirect Purchase Reverse Engineering	Improve Military Discover Countermeasures Gain Power
Terrorists	Theft of MCT Materials Indirect Purchase	Difficult to manufacture WMD Gain Power
Black Marketeers	Theft of MCT Materials Indirect Purchase	Profit

TABLE 2. SEEKERS OF MCT

U.S. military technology is envied by all militaries seeking to raise their level of sophistication. Often our MCT can be stolen, purchased, or taken apart and examined (reverse engineering).

Other seekers of MCT typically do not have the capability to manufacture complex systems, finding it easier to steal or buy MCT through a middleman. The MCT market can be very lucrative for owners or resellers of MCT.

The success of the U.S. in maintaining MCT secrets can be described as marginal at best. Figure 1 demonstrates that the lure of money, patriotism, or job dissatisfaction have encouraged numerous Americans to betray their country. Perhaps the most famous case of MCT espionage was Julius and Ethel Rosenberg being executed in 1953 for giving away our atomic bomb technology to the Soviets. Other spies such as Aldrich Ames, Jonathan Pollard, Earl Pitts, Harold Nicholson, and Robert Hanssen all serve as reminders that the threat is active and real. Most recently, Brian Regan, a former Air Force intelligence analyst, was convicted of giving technical information on our spy satellites to China and Iran.[2] These cases serve as reminders that we must safeguard our MCT with the utmost urgency and understand that our potential adversaries are highly skilled in espionage activities.

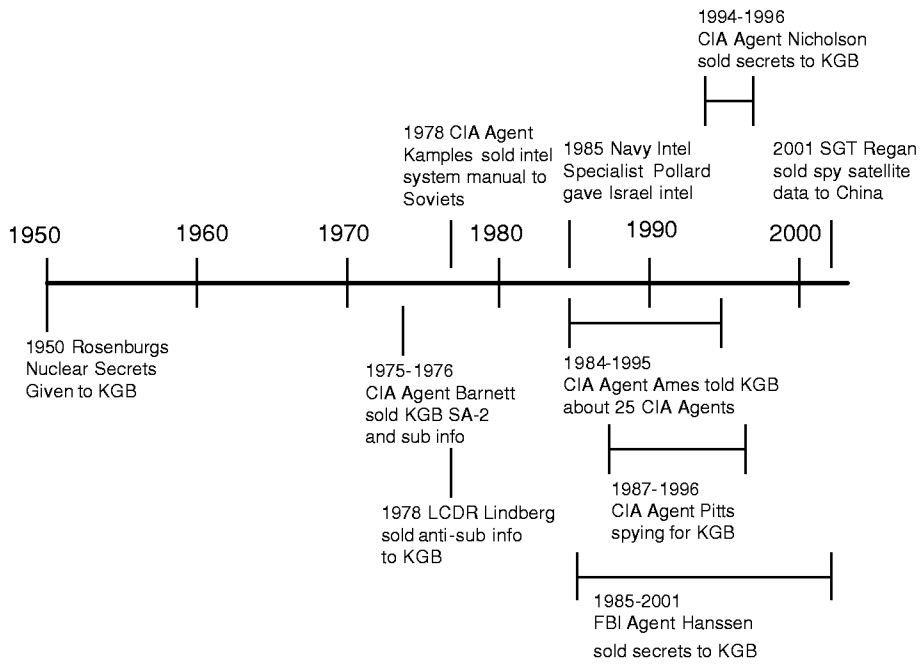

FIGURE 1. TIMELINE OF US SPYING CASES

The DoD goal is to protect U.S. technology from unauthorized access without affecting competition, innovation, or economic growth.[3] Technology can be in the form of an end

product, repair parts, blueprints, drawings, manuals, computer software, instructions, online documents, or a contractor bid. The Under Secretary of Defense for Research and Engineering is tasked with the implementation of DoD Directive 5230.25, which monitors U.S. contractors to see if they have violated U.S. export laws or their security certification.[4] The number of critical technologies, the numerous forms of data, and the methods by which MCT information can be transferred make securing MCT a very challenging problem. Protecting MCT requires personnel who are well trained, technically proficient, and aware of our potential enemies' capabilities.

DoD recognizes that we must transform how we integrate our military power with the other instruments of nation power. "Integration of national power is especially critical for overcoming terrorist or other unconventional adversaries that cannot be defeated by military means alone. Enhanced coordination among agencies and across all levels of government (federal, state, local) will promote increased cooperation, more rapid response, and the ability to conduct seamless operations."[5] How to improve our government's task organization to protect MCT is the primary focus of this paper. The new organization must be efficient and streamlined.

ANALYSIS

Another problem area is securing technology that has a military application as well as a non-military application. These are known as dual-use technologies, which further complicates the DoD goal of protecting U.S. technology. A recent study concluded that 38% of all illegal technology transfers were dual-use technologies, mainly in the area of high performance computers, laser mirrors, and oscilloscopes.[6] In recognition of this growing problem, the U.S. along with 32 other countries signed the Wassenaar agreement in 1996 to provide each other information on transfers of conventional arms and dual-use technologies. The problem with this agreement is that there are no punitive clauses and China did not sign this agreement. Widely available commercial technologies such as information technology, high resolution imagery, and global positioning systems will improve the disruptive and destructive capability of any potential adversary.[7]

The National Security Strategy of Engagement and Enlargement (1995) was President Clinton's directive to link DoD, DoE, and the intelligence community into a coherent science and technology strategy. The directive states: "Technological superiority underpins our national military strategy, allowing us to field the most potent military forces by making best use of our resources, both economic and human. It is essential for the U.S. to maintain superiority in those technologies of critical importance to our security."[8] With annual funding of over $100 million,

the directive emphasizes the use of sensors to counter weapons of mass destruction (WMD), information technologies to digitize the battlefield, and science and technology to combat terrorism. This directive is a landmark in protecting MCT and serves as an excellent starting point to discuss further improvements. In 2002, a G-8 agreement pledged $20 billion to increase support for nonproliferation and threat reduction programs.[9] President Bush's 2002 National Security Strategy proposes the integration of MCT protection into the homeland security program, but no specifics have been published.

There exists a dichotomy between the transfer of technology and security. Technology is one of the key factors in the growth of economic and military power. "The interaction of technology, economy, and war has been characterized as a defining feature in international relations and a determinative factor in the rise and fall of great powers."[10] The transfer of technology should be weighed against military/strategic considerations, since maintaining a superior capability over our potential adversaries is critical to national security. Technology does not have to be directly used to improve military capabilities, instead a new technology could free up resources that can be used in new military production. A delicate balance must be maintained between the transfer of technology and the need for security.

Using spies is the traditional way to steal technology, but our potential adversaries have become more inventive in their information gathering methods. A novel example is where a Western European government sent out invitations to U.S. defense contractors to bid on a contract for an avionics system. The West European government decided to build its own system after reviewing the detailed proposals. Later a U.S. contractor saw their copied design at a trade show.[11] Requests for information to knowledgeable U.S. persons may come in the form of email, fax, or telephone, often asking for help in answering a research question. If not properly briefed, most persons would answer as if a lost person were asking for directions.[12] If the need is great enough, a potential adversary could simply purchase a U.S. company through a third party to gain the desired technology.[13] Foreign engineers could also seek employment at a U.S. company in an attempt to gain knowledge. In this era of increasing globalization, foreign markets can easily be exploited for information gathering.

The Internet is the fastest and easiest way for potential adversaries to collect MCT information.[14] There are numerous advantages in gathering information via the Internet. The Internet can cover a variety of sources at tremendous speeds, with little risk of detection. Improved search engines, databases, electronic bulletin boards, government sites, and electronic journals make it easy to find information with a few keystrokes. Potential adversaries can attack from their home base and use hosts within their own country to hide their identity.

Foreign security services are becoming more computer savvy, such as using eavesdropping programs to monitor Internet traffic. Files or passwords can be intercepted and later used to gain access to classified sites. Low cost and risk with a potential for high payoff makes the Internet an attractive medium in which to collect MCT data.

Qualitative Risk Analysis examines the threats (things that can attack the system), vulnerabilities (makes an attack more likely to succeed), and controls (countermeasures for vulnerabilities). A risk analysis tries to take a snapshot of our potential vulnerabilities. Most of the analysis thus far in this paper has focused on the threats. A situation requiring immediate attention is China's efforts in monitoring U.S. operations in Iraq. The results of the war have reinforced China's desire to speed the acquisition of information technology and weapons mobility.[15] In addition, China is enhancing its satellite tracking network and is building lasers to blind low orbiting satellites.[16] Low orbiting satellites provide high resolution photographs, which can be used to help determine troop concentrations and deployment status. The Chinese government's 863 program is designed "to acquire and develop technology in a number of areas to include machine tools, electronics, petrochemicals, electronic information, bioengineering, nuclear research, aviation, and space."[17] China's 863 program has an monitoring station in the Caribbean masquerading as an economic development office. It is quite odd that this station is only manned when there are space launches from Cape Canaveral. Based on these observations, it is apparent that U.S. MCT is under attack from a coordinated and determined potential adversary, whose goal is to become a world-class military in 10-15 years.

There are numerous vulnerabilities in the protection of MCT. Our open society promotes the free exchange of ideas and the Internet makes information access easy. MCT is a diverse collection of technologies created by multinational corporations with thousands of employees. For example, Intel has over 50,000 dealers worldwide and 60% of their revenues come from overseas business.[18] We have numerous allies that utilize U.S. MCT that are not under U.S. control. Complex weapons systems have parts produced outside the U.S., such as the optical glass in reconnaissance satellites made in Germany, semiconductor satellite chips from Japan, and parts of the Abrams gunner sight made in Italy.[19] Recognizing vulnerabilities becomes the first step in the development of controls. We have to realize that today's global economy makes it difficult to produce a product that is 100% made in the U.S.

There exists a vast array of controls to protect MCT. DoD utilizes DoD Directive 5230.25 to give guidelines to contractors on the importance of protecting MCT. The directive contains the requirements to obtain export licenses to release any technical data and procedures on

reporting possible compromises of MCT.[20] The Defense Security Service (DSS) was formed to improve risk management in industry classified programs, threat awareness, deterrence of illegal technology transfers, and facilitating the prevention of economic espionage in defense contractor facilities.[21] DSS examines who is targeting us, what is being targeted, and what methods are being used. DSS also examines trends in information collection and activity by foreign companies and governments against U.S. industries. DSS is one of the key government agencies associated with the protection of MCT. Unfortunately, there is little evidence of the DSS working outside the DoD in the protection of MCT.

The recently formed DoHS has started initial steps in organizing inter-agency coordination of MCT protection. In coordination with the Department of State, every diplomatic post was sent the MCT list with a list of states that sponsor terrorism. Consular officers were instructed to become familiar with MCT keywords and phrases when listening to answers to interview questions.[22] Instructions were given that special attention should be paid to applicants who wish to conduct research in MCT and special paperwork needs to be done if the applicant is from a state that sponsors terrorism. While consular officers do not have the expertise to ask detailed questions about MCT, this example of the Department of Homeland Security working with DoD and the Department of State to mobilize the government in MCT protection is promising. The Department of State can serve as our first line of defense by limiting MCT traffickers access into the country.

Export controlled information and material is managed by the Department of State for International Traffic in Arms Regulation (ITAR) and the Department of Commerce for items in the Export Administration Regulation (EAR). The purpose of ITAR and EAR is to prevent foreign citizens, industries, or governments from obtaining information that can be used against U.S. security interests.[23] Unfortunately, there are confusing rules depending if the applicant is a U.S. citizen, an immigrant alien with a green card, or a foreign national. The U.S. Immigration and Customs Enforcement's (now part of the Department of Homeland Security) Project Shield America is part of the national security strategy of preventing illegal exports of MCT. Project Shield America is a three prong effort of inspection/interdiction at high threat ports, investigations of violators of ITAR and EAR, and international cooperation.[24] This confusing state of interagency spans of control serves as an example of why MCT protection needs a new organization.

The objectives, methods, and resources used in protecting MCT are out of balance. While the objectives are clearly stated in the National Security Strategy and National Military Strategy, the methods to accomplish these objectives are disjointed and uncoordinated. The

numerous government agencies involved in the process represent tremendous resources, but what is needed is a clear, coherent plan with a unity of effort and command. Failure to adequately protect MCT will erode the U.S. advantages in technical superiority and could compromise U.S. forces in the next conflict.

Critics of the current state of MCT protection declare that there are deficiencies in the enforcement of norms, export controls, and national export systems.[25] Since the U.S. took the lead during the Cold War in enforcing export controls to the Soviet bloc, the U.S. should take the international lead in multilateral export control coordination and further improve national export controls.[26] Lincoln Bloomfield, Department of State Assistant Secretary for Political Military Affairs acknowledged that if Al-Qaeda can move freely in and out of 68 countries, there is little confidence that our system can control illicit exports.[27] On a positive note, licensing of exports has been streamlined and greater cooperation arrangements have been made with the United Kingdom, Australia, and Canada. The Assistant Secretary stated our national export systems must be water-tight and that the Bush administration recognizes the need to balance the non-proliferation goal with maintaining the quality of the defense industry.[28]

Our advantages in science and technology are necessary in the securing the homeland. A systematic national effort is required to harness the complex mix of companies, universities, research institutions, and government labs into a national focus.[29] The DoHS has been tasked by the President for the following initiatives:

- Develop chemical, biological, radiological, and nuclear countermeasures
- Develop systems for detecting hostile intent
- Apply biometric technology to identification devices
- Coordinate research and development of the homeland security apparatus
- Establish a national lab for homeland security
- Conduct demonstrations and pilot deployments[30]

The entire thrust of the DoHS strategy is to use science and technology to win the war on terror. However, there are no plans outlined in the DoHS strategy for protecting MCT from potential adversaries.

One of the most damaging reports on the current state of MCT protection was issued by the General Accounting Office (GAO) in April 2004. The report states that "U.S. export regulations governing China contain inherent inconsistencies and are based on outdated government assessments of the availability of technology from non- U.S. sources."[31] The report

also stated that the Commerce Department was unable to focus its efforts and that the DoD had not conducted required studies of the effect of exports of advanced semiconductor manufacturing equipment on national security. [32] The report highlights the current system is not working and immediate changes need to be implemented. The report also highlights our apparent deficiencies because now we are selling our MCT as well as letting China's 863 program steal our MCT.

U.S. companies have voiced concern that current export license requirements are hurting revenues.[33] In order to improve the situation, the Department of Commerce traveled to China to conduct 20 high-priority inspections on dual-use technologies to see if these items are being properly used.[34] These dual use inspections seem to be mainly for show, since the U.S. is interested in improved relations with China. After the inspection, the MCT dual-use items could be converted back to illegal uses or could be reverse engineered and then copied. Increased resources should be devoted to the monitoring of dual-use items.

The current state of MCT protection, the duplication of effort, and the non-unity of command suggests that an immediate reorganization of government efforts is required. Too often our government makes drastic changes only after a catastrophic event such as a 9-11 occurs. A good example of a significant reorganization based on a catastrophic event is the Intelligence Reform Bill of 2004. We should not wait until such a scenario as described in the introduction of this paper occurs. Our technological edge in our military must be protected and maintaining this edge is of vital national concern. There are three basic courses of action in the reorganizing of MCT protection:

COURSE OF ACTION A

Maintain current government organization for protecting MCT

Advantages:

+ No government reorganization required, maintains status quo
+ No new costs
+ Easy to implement

Disadvantages

- Does not address current MCT protection problems
- Does not meet the spirit of the Homeland Security Strategy
- Does not recognize our enemies improving capabilities
- Continues the current state of non-unity of effort

COURSE OF ACTION B

Make the DSS the lead agency for protecting MCT and integrate into the DoHS

Advantages:

+ Takes advantage of DoHS organization to improve interagency cooperation
+ Improves information sharing
+ Maintains unity of command
+ Maintain DSS expertise and experience in MCT protection areas
+ Incorporates reorganization ideas modeled on the Intelligence Reform Bill

Disadvantages

- Requires new lines of communication
- Requires many agencies to lose spheres of influence
- High initial startup costs
- Will required detailed planning and oversight to implement
- Requires Congressional Legislation

COURSE OF ACTION C

Create a new agency for protecting MCT.

Advantages:

+ Recognizes the MCT protection problem
+ Improved information sharing
+ Meets the spirit of the Homeland Security Strategy
+ Personnel and funding dedicated to MCT protection

Disadvantages

- Does not take advantages of the in place government structures and DSS expertise and experience
- Expands duplication of effort and overlap of resources
- Requires Congressional legislation
- High startup costs
- Creates a new government agency

RECOMMENDATIONS

The importance of MCT protection and the nation's weak record on protecting MCT dictates that drastic action is required. The course of action selected should meet our pressing requirements, utilize existing organizations, and take advantage of the personnel with experience and technical knowledge in dealing the protection of MCT. The guidelines outlined

by the 9-11 Commission in the reorganization of our intelligence assets serve as an excellent blueprint for the reorganization of government assets in the protection of MCT. This paper recommends implementing COA B with the following guidelines:

1. Assign DoHS as the lead federal agency in the protection of MCT. This would insure unity of command among numerous government agencies (DoD, Commerce, Energy, State, Customs) and avoid duplication of efforts and resources. The DoHS was formed for the purpose of merging government functions. This is done through an interagency process coordinated by the White House. Congress may feel out of the loop, but they should use their traditional power of the purse as clout.[35]

The DoD's DSS should form the core of the DoHS spearhead for protecting MCT. DSS has the experience and technological expertise to take lead in this interagency effort. Merging DSS with DoHS would give DSS the necessary framework to become a more interagency organization. Many of reforms recommended by the 9/11 Commission enacted in the Intelligence Reform Bill of 2004 have interesting parallels that should be applied to protecting MCT:

- Creates the Director of National Intelligence, a principle advisor to the President who coordinates the nation's spy agencies
- Establishes a National Counterterrorism Center for planning intelligence and coordinating information
- Provides funds to combat money laundering and financial crimes
- Establishes mandatory minimum sentences for possessing or trafficking in missile systems built to destroy aircraft
- Requires a national transportation security strategy, including advanced airline passenger prescreening and biometric identification system[36]

Like the intelligence reform plan, a director for protecting MCT insures unity of command across numerous government agencies. A principle advisor to the President would also focus attention on the MCT protection problem. Figure 2 demonstrates the agencies involved in this effort and proposed lines of communication. A national center for protecting MCT would greatly improve information flow and give much needed structure to a growing problem. A central point would also make it easier for our allies to focus their efforts. More funding and mandatory sentencing incorporated in the Intelligence Reform Bill of 2004 should be applied to MCT traffickers, resulting in a similar detrimental affect on our adversaries. The DSS has a strategy for the protection of MCT, it should be expanded to incorporate a complete interagency effort. A 9/11

type disaster should not be necessary for the government to reform itself into a more efficient organization.

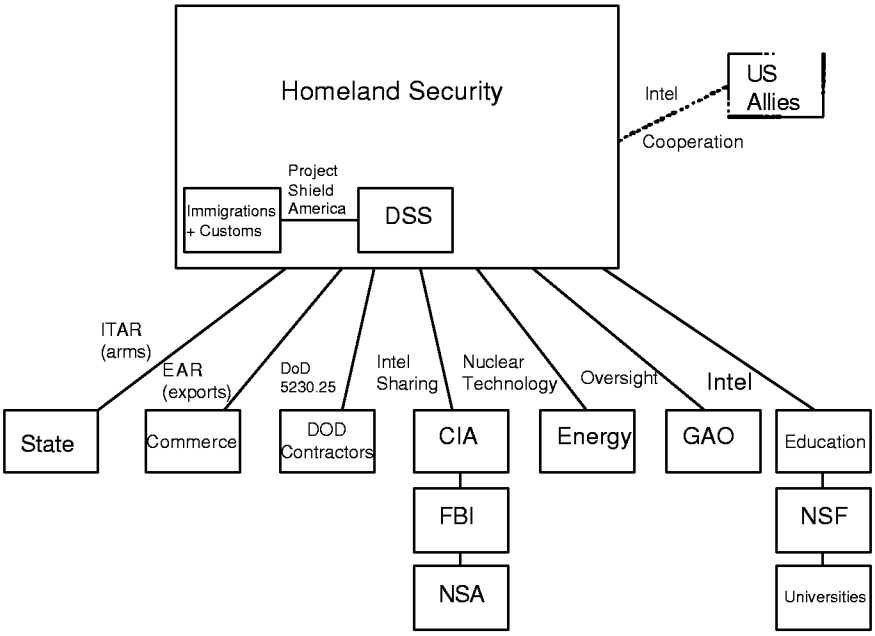

FIGURE 2. NEW ORGANIZATION FOR PROTECTING MCT

2. Incorporate the sharing of intelligence. The DoHS is now working with the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the National Security Agency (NSA) in the sharing of intelligence. If the FBI, CIA, or NSA discover any keywords or information on MCT, it should be relayed to the experts on MCT, the DSS. Emphasis should be placed on MCT information collection. The FBI, CIA, and NSA also have outstanding resources to monitor computer attacks, eavesdropping, and illegal access. While these agencies do not have the technical expertise for MCT monitoring, the information gathered could prove very useful. The Intelligence Reform bill greatly improves our intelligence gathering abilities, many of which can be used to improve MCT protection:

- Adds 2,000 Border Patrol agents and 800 immigration officers every year for the next five years.
- Use of advanced sensors, videos, and unmanned aircraft to survey borders
- An early future requirement for biometric screening for all visitors
- Strengthened visa requirements

- Grants wiretapping and investigative authority to pursue "lone wolf" terrorists[37]

The Intelligence Reform bill will have the direct and indirect effect of improving the protection of MCT. The bill will make it more difficult to traffic in illegal MCT and limit access into the country of seekers of MCT. The Intelligence Reform Bill is an excellent start in improving MCT protection, building on this framework is necessary in order for our military to maintain its technological advantages. Figure 2 demonstrates that many government agencies have an existing area of expertise in MCT protection, with a reorganization creating a new interagency synergy very similar to the Intelligence Reform Bill reorganization.

3. Expand the Export-Controlled Technology oversight at Contractor, University, and Federally Funded Research and Development Center Facilities. Persons wishing DoD funding in the future will have to comply with the rules enforcing protection of MCT.[38] This should be expanded to other federal programs in the National Science Foundation (NSF) and the Department of Education, since academia is one of the main producers of MCT. In the world of academia, conferences are held to discuss solutions to problems and proceedings are published. A conference should be held to address the protection of MCT in academia, with all major university presidents being invited. In the post 9-11 world, interest would be high. Our National Military Strategy recognizes that technology diffusion and access to advanced weapons can have significant implications for our military capabilities.[39] Only by recognizing that MCT comes from numerous areas ensures that a different strategy is required for each area of MCT creation.

4. Improve cooperation with allies in the protection of MCT. It is in our allies' interest to keep MCT out of the hands of rouge states and non-state actors. MCT availability facilitates the easier production of WMD. The relative availability of MCT, unemployed scientists, and terrorist organizations cooperating with rouge states puts the WMD threat into a special category.[40] Possession of WMD gives a terrorist organization new global power that they desperately seek. Our government now realizes that terrorists are strategic actors who are working on obtaining WMD to wreak unprecedented damage on our country.[41] Good cooperation already exists for WMD monitoring; this must be expanded for MCT.

Some undesired effects could result from these recommendations. Due to the open nature of academia, any requests for reporting could be met with resistance. Export restrictions could stifle U.S. companies, so the DoHS must be responsive and staffed with the required technical expertise so that legal export transactions can be rapidly approved. Companies may not wish to do extra security, because it will increase costs. MCT protection requires the

cooperation of many government agencies, some of which may not wish to cooperate due to loss of prestige or power.

Only a team effort from all branches of the government, industry, academia, and our allies will effectively protect MCT. While protecting MCT is a complex problem, a multilayered approach will greatly improve the national strategic goal of protecting MCT. The 9/11 Commission's report serves as a excellent model that should be adopted so that our best minds can recognize the problems associated with protecting MCT and identify how innovative solutions can be developed. We must be fully prepared to win the nation's next war, which means we must make every effort to protect our MCT.

WORD COUNT=4794

ENDNOTES

[1]Department of Defense, *Military Critical Technology List, Section 17: Information Security Technology* (Washington, D.C.: Defense Threat Reduction Agency, October 2003), iii.

[2]Jerry Markon, "FBI Finds Documents in Spy Case; Papers, CDs Called 'Damaging' to U.S," *The Washington Post*, 29 July 2003.

[3]Aviation Engineering & Product Support, "Military Critical Technology," 4 November 2003; available from <http://www.mavicp.navy.mil.07/military _critical_technology.htm>; Internet; accessed 20 September 2004.

[4]Department of Defense, *Withholding of Unclassified Technical Data from Public Disclosure, Directive 5230.25* (Washington, D.C.; Department of Defense, 18 August 1995), 7.

[5]Department of Defense, *Transformation Planning Guidance* (Washington, D.C.; Department of Defense, April 2003), 7.

[6]Defense Security Service, "Illegal Technology Transfer," 4 June 2001; available from <http://www.dss.mil/search-dir/training/csg/security/T1threat/Techtran.htm>; Internet; accessed 20 September 2004.

[7]Joint Chiefs of Staff, *National Military Strategy of the United States of America 2004* (Washington D.C.; 2004), 6.

[8]Clinton White House, "Maintaining Military Advantage Through Science and Technology Investment," 1995; available from ,http://clinton1.nara.gov/White_House/EOP/OSTP /nssts/html/chapt2.html>; Internet, accessed 20 September 2004.

[9]White House, *The National Security Strategy of the United States of America* (Washington D.C., September 2002), 14.

[10]Jing-Dong Yuan, "The Future of Export Control: Developing New Strategies for Nonproliferation," International Politics 39: Kluwer Law Interational, (June 2002): 133.

[11]Defense Security Service, "Use of Contract Bidding to Elicit Information," 11 July 2003; available from <http://www.dss.mil/cithreats/contrbid1.htm>; Internet; accessed 20 September 2004.

[12]Defense Security Service, *Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed Against the U.S. Defense Industry* (Washington, D.C.: Public Release #981210-06, 11 July 2003), 2.

[13]Ibid, 3.

[14]Defense Security Service, "Internet: The Fastest Growing Modus Operandi for Unsolicited Collection," available from <http://www.dss.mil/cithreats/internet.htm>; Internet; accessed 20 September 2004.

[15]The Conservative Caucus, "Red Chinese Military Threat & Technology Transfers," available from <http://www.conservativeusa.org/redchina-missile.htm>; Internet; accessed 20 September 2004.

[16]Ibid, 3.

[17]Ibid, 10.

[18]Yuan, 141.

[19]Steve Eastburg, *America's Eroding Critical Technology Base* (Program Manager, January-February 1995), 22.

[20]Department of Defense, 4.

[21]Defense Security Service."Counterintelligence," available from <http://www.dss.mil/cithreats/index.htm>; Internet; accessed 20 September 2004.

[22]Secretary of State, "Technology Alert List Update," Electronic mail message to all Diplomatic and Consular Posts, 1 August 2002.

[23]Defense Security Service, "Export Controlled Information," available from <http://www.dss.mil/search-dir/training/csg/security/S2unclas/Export.htm>; Internet;, accessed 16 September 2004.

[24]U.S. Immigration and Customs Enforcement, "Project Shield America," available from <http://www.ice.gov/graphics/investigations/nationalsecurity.shiledAmerica.htm>; Internet; accessed 16 September 2004.

[25]Yuan,143.

[26]Yuan, 147.

[27]Lincoln Bloomfield, "Globalization of Export Controls and Sanctions," *DISAM Journal* (Winter 2001-2002): 53.

[28]Ibid, 53.

[29]Office of Homeland Security. 51

[30]Ibid. 51-54..

[31]Nadine Siak, "Government Investigators Find Export Control Policy, Practices Flawed," available from <http://japan.usembassey.gov/e/p/tp-ec0543.html>; Internet; accessed 6 October 2004.

[32]Ibid,2.

[33]David Friedman, "Of Commerce & Warfare; The Belief that Military Technology can be Shielded in Commercial Deals is Sheer Fantasy," *Los Angeles Times*, 28 June 1998, p.1.

[34]Bruce Odessey, "Export Controls Aimed at China Facing Administration Opposition," available from <http://usinfo.state.gov/is/Archive/2004/May/20-503148.html>; Internet; accessed 6 October 2004.

[35]William Newmann, "Reorganizing for National Security and Homeland Security," *Public Administration Review*, Vol. 62, (2001): 351.

[36]Associated Press, "Congress Approves Sweeping Intelligence Reform," available from <http://www.msnbc.msn.com/id/6655348/>; Internet; accessed 27 December 2004.

[37]Department of Defense, Export Controls: Export-Controlled Technology at Contractor, University, and Federally Funded Research and Development Center Facilities (Washington, D.C.; Department of Defense, 25 March 2004), 1.

[38]Chairman of the Joint Chiefs , National Military Strategy of the United States of America 2004 (Washington, D.C.; Chairman of the Joint Chiefs, 2004), 6.

[39]Office of the President, *National Strategy for Combating Terrorism* (Washington, D.C.; Office of the President, February 2003), 10.

[40]Office of Homeland Security, *National Strategy for Homeland Security* (Washington, D.C.; Office of Homeland Security, July 2002), vii.

[41]Ibid., viiii.

GLOSSARY

CIA	Central Intelligence Agency
DoD	Department of Defense
DoE	Department of Energy
DoHS	Department of Homeland Security
DSS	Defense Security Service
EAR	Export Administration Regulation
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
GPS	Global Positioning System
ITAR	International Traffic in Arms Regulation
MCT	Military Critical Technology
NSA	National Security Agency
NSF	National Science Foundation
SRP	Strategic Research Project
WMD	Weapons of Mass Destruction (Nuclear, Biological, Chemical)

BIBLIOGRAPHY

Associated Press. "Congress Approves Sweeping Intelligence Reform." 8 December 2004. Available from <http://www.msnbc.msn.com/id/6655348/>. Internet. Accessed 27 December 2004.

Aviation Engineering & Product Support. "Military Critical Technology." 4 November 2003. Available from <http://www.mavicp.navy.mil.07/military _critical_technology.htm>. Internet. Accessed 20 September 2004.

Bloomfield, Lincoln. Jr. "Globalization of Export Controls and Sanctions." *DISAM Journal*. (Winter 2001-2002): 52-56.

Chairman of the Joint Chiefs. *National Military Strategy of the United States of America 2004*. Washington D.C.; 2004.

Clinton White House. "Maintaining Military Advantage Through Science and Technology Investment." Available from <http://clinton1.nara.gov/White_House/EOP/OSTP /nssts/html/chapt2.html>. Internet. Accessed 20 September 2004.

Defense Daily International. "Lockheed Sees Blanket JSF Export License By Year's End, Deemed Export at Issue." *Potomac* Vol. 2, Issue 25 (26 April 2002): 1.

Defense Daily International. "AIA, EIA, NDIA Call on Bush to More Rapidly Reform Export System." *Potomac* Vol. 3, Issue 14 (8 February 2002): 1-2.

Defense Daily International. "War on Terror Fuels Need for Export Reforms, Multilateral Approach." *Potomac* Vol. 2, Issue 40 (26 October 2001): 1-4.

Defense Daily. "Administration Protest Proposed Export Restrictions." *Potomac* Vol. 222, Issue 38 (24 May 2004): 1-2.

Defense Security Service. "Illegal Technology Transfer." 4 June 2001; Available from <http://www.dss.mil/search-dir/training/csg/security/T1threat/Techtran.htm>. Internet. Accessed 20 September 2004.

Defense Security Service. "Counterintelligence." 11 July 2003; Available from <http://www.dss.mil/cithreats/index.htm>. Internet. Accessed 20 September 2004.

Defense Security Service. "Scholarly Approaches to Collect Scientific and Technical Information from Cleared Defense Companies." 11 July 2003. Available from <http://www.dss.mil/cithreats/satest.htm>. Internet. Accessed 20 September 2004.

Defense Security Service. "Use of Contract Bidding to Elicit Information." 11 July 2003. Available from <http://www.dss.mil/cithreats/contrbid1.htm>. Internet. Accessed 20 September 2004.

Defense Security Service. "Internet: The Fastest Growing Modus Operandi for Unsolicited Collection." 11 July 2003. Available from <http://www.dss.mil/cithreats/internet.htm>. Internet. Accessed 20 September 2004.

Defense Security Service. *Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed Against the U.S. Defense Industry*. Washington, D.C.: Public Release #981210-06, 11 July 2003.

Defense Security Service. "Who's Doing What to Whom ?." 4 June 2001. Available from <http://www.dss.mil/search-dir/training/csg/security/T1threat/Intro.htm>. Internet. Accessed 16 September 2004.

Defense Security Service. "Export Controlled Information." 1 June 2001. Available from <http://www.dss.mil/search-dir/training/csg/security/S2unclas/Export.htm>. Internet. Accessed 16 September 2004.

Defense Security Service. "Militarily Critical Technologies List." 30 April 2001. Available from <http://www.dss.mil/search-dir/training/csg/security/T1threat/Metl.htm>. Internet. Accessed 16 September 2004.

Department of Defense. *Withholding of Unclassified Technical Data from Public Disclosure*, Directive 5230.25. Washington, D.C.; Department of Defense, 18 August 1995.

Department of Defense. Export Controls: Export-Controlled Technology at Contractor, University, and Federally Funded Research and Development Center Facilities. Washington D.C.; Department of Defense, 25 March 2004.

Department of Defense. *Transforming Planning Guidance*. Washington, D.C. Department of Defense, April 2003.

Department of Defense. *Military Transformation*. Washington, D.C. Department of Defense, Fall 2003.

Department of Defense. *Military Critical Technology List, Section 17: Information Security Technology*. Washington, D.C.: Defense Threat Reduction Agency, October 2003.

Eastburg, Steve. "America's Eroding Critical Technology Base." *Program Manager,* January-February 1995, 22-24.

Friedman, David. "Of Commerce & Warfare; The Belief that Military Technology Can Be Shielded in Commercial Deals is Sheer Fantasy." *Los Angeles Times*, 28 June 1998.

Hicks, Donald. "U.S. – China Security Review Commission." 17 January 2002. Available from <http://www.uscc.gov/textonly/trascriptstx/teshic.htm>. Internet. Accessed 6 October 2004.

Joint Chiefs of Staff. *National Military Strategy of the United States of America 2004*. Washington D.C.; 2004.

Juster, Kenneth. "2003 Export Controls & Policy Conference." 20 October 2003. Available from <http://www.cwc.gov/Industry_Outreach/speeches_and_pressreleases/Kenneth_Juster_keynote>. Internet. Accessed 6 October 2004.

Markon, Jerry. "FBI Finds Documents in Spy Case; Papers, CDs Called 'Damaging' to U.S." *The Washington Post*, 29 July 2003.

Miller, Judith. "U.S. Asks Putin Not to Sell Iran A Laser System." *New York Times,* 19 September 2000.

National Research Council. *Star 21 Strategic Technologies for the Army of the 21st Century.* Washington: National Academy Press, 1992.

National Research Council. *Star 21 Mobility Systems.* Washington: National Academy Press, 1992.

National Research Council. *Star 21 Special Technologies and Systems.* Washington: National Academy Press, 1992.

Newmann, William. "Reorganizing for National Security and Homeland Security." Public Administration Review Vol. 62, (2001): 127-133.

"Not a Death Case." *The Washington Post* (13 May 2002): A14.

Odessey, Bruce. "Export Controls Aimed at China Facing Administration Opposition." 20 May 2004. Available from <http://usinfo.state.gov/is/Archive/2004/May/20-503148.html>. Internet. Accessed 6 October 2004.

Office of Homeland Security. "National Strategy for Homeland Security." Washington D.C.; July 2002.

Office of Management and Budget. "Military Critical Technology Budget." Washington D.C.; February 2004.

Office of the President. "National Strategy for Combating Terrorism." Washington D.C.; February 2003.

Pomfret, John. "China Wary of Weapons Searches; Official: Country Won't be Transit Point for North Korean Arms." *The Washington Post*, 23 August 2003.

Richtel, Matt. "Spy Cases Target China." *New York Times*, 16 January 2003.

Sanger, David. "The North Korean Uranium Challenge." *New York Times*, 24 May 2004.

Secretary of State. "Technology Alert List Update." Electronic mail message to all Diplomatic and Consular Posts. 1 August 2002.

Siak, Nadine. "Government Investigators find Export Control Policy, Practices Flawed." 2004. Available from <http://japan.usembassey.gov/e/p/tp-ec0543.html>. Internet. Accessed 6 October 2004.

The Conservative Caucus. "Red Chinese Military Threat & Technology Transfers." 2004. Available from <http://www.conservativeusa.org/redchina-missile.htm>. Internet. Accessed 20 September 2004.

U.S. Immigration and Customs Enforcement. "Project Shield America." Available from <http://www.ice.gov/graphics/investigations/nationalsecurity.shiledAmerica.htm>. Internet. Accessed 16 September 2004.

Wall, Robert. "Closer Watch: U.S. Intends to Enhance Controls Over Missile and UAV Technologies." *Aviation Week & Space Technology*, 15 March 2004.

White House. The National Security Strategy of the United States of America. Washington D.C.; September 2002.

Yuan, Jing-Dong. "The Future of Export Control: Developing New Strategies for Nonproliferation." *International Politics* 39 (June 2002): 131-151.